6-15-2000

Hot Topic: The Legislature Sends Message to Cities with Electronic Mail: You Must Have a Written E-mail Policy

Sid Hemsley
Municipal Technical Advisory Service

Hot Topics for Tennessee cities and towns

June 15, 2000 #55

The Legislature Sends Message to Cities with Electronic Mail: You Must Have a Written E-mail Policy

By Sid Hemsley
MTAS Legal Consultant

On or before July 1, 2000, most Tennessee governments — including cities — that operate or maintain an electronic-mail (e-mail) system must adopt a written policy about monitoring e-mail communications.

The policy must include:

- the circumstances that warrant e-mail monitoring; and
- a statement that the employee's e-mail correspondence may be a public record under Tennessee's Public Records Law and may be inspected by the public (Tennessee Code Annotated (T.C.A.) § 10-7-512).

The statute, adopted in 1999, does not require a city to monitor e-mail; that is each municipality's decision. If a city chooses to monitor e-mail, its policy must meet both conditions stated above. In a municipality that does not monitor e-mail, however, the policy must at least satisfy the public record statement requirement. Attachment I is a sample policy that addresses legal and other personnel matters for cities that monitor e-mail.[1] A few of those issues will be briefly discussed in this Hot Topic. Those and related topics will be covered more thoroughly in a future MTAS Technical Bulletin.

Should the city monitor e-mail?

City officials and employees who must answer the question of whether or not to monitor e-mail should review the following reasons.

Some of the reasons **not** to monitor include:

- the practice may be seen as intrusive and obnoxious;
- it generates distrust between management personnel and employees, and even among fellow employees;
- monitoring may be expensive, particularly the cost of retrieving deleted e-mail; and
- monitoring involves some serious legal privacy issues that apply generally to all government employees.

Some of the reasons **for** monitoring include:

- improper misuses of e-mail could have serious legal and financial repercussions for the city, such as the disclosure of medical or other confidential files or information;
- remarks or jokes disseminated and forwarded by e-mail that may have been intended to be harmless could be grounds for a suit against the city for creation of a hostile work environment, for racial, religious, or sexual discrimination, or even for libel or defamation;
- software owned by the city may be used to conduct non-city business; or
- software may be duplicated illegally for home or other use, which might constitute software piracy copyright infringement.

In addition, e-mail is subject to the discovery rules in litigation.

What are the major problems involved in monitoring e-mail?

The General Assembly pointed to problems in monitoring e-mail. In adopting T.C.A. § 10-7-512, it directed that an e-mail study be conducted "to balance the privacy interests and practical limitations of public officials and employees, with the public policy interests in access to government information." The General Assembly said that the use of e-mail by governments creates the following "unique circumstances." Generally, telephonic communications are not stored in any form and are regarded as private, but e-mail creates an electronic record that may be used or retrieved in paper format; and e-mail is becoming more common and important, but public officials are not equipped to act as official custodians of such communications and to determine whether or not the communications might be public records. Certain federal and state statutes and case law also protect the privacy of workplace e-mail communications.

How does the city handle the privacy problem?

Generally, the statutes and the cases that protect the privacy of e-mail in the government workplace permit monitoring of such e-mail where the government employees have been given notice that their e-mail communications are subject to being monitored. The most successful notice is a written notice. For that reason, the city can ensure that the e-mail policy it adopts in accordance with T.C.A. § 10-7-512 includes provisions notifying employees that the city intends to monitor e-mail. Employees should be required to read the policy and to acknowledge with their signature that they understand it. Attachment II contains a sample acknowledgment statement.

How does the city handle the open records problem?

T.C.A. § 10-7-512 does not require city's to monitor its e-mail. However, if the city decides not to monitor, the policy must include the statement that employee's e-mail correspondence may be a public record under Tennessee's Public Records Law (T.C.A. § 10-7-503), and subject to inspection under "this part." The "this part" phrase suggests that a person claiming access to a city's e-mail might base his or her claim under both Tennessee's Public Records Law and T.C.A. § 10-7-512.

Most municipal records are open under T.C.A. § 10-7-503, but that law contains several exceptions, including some found expressly in the law, as well as some found in other state and federal laws. Generally, a city can answer the question of whether a particular e-mail message or document is open or closed by determining whether the "hard copy" of the same e-mail message or document would be open or closed under the law. The answer to some of these questions will be obvious, while

others will require thought and even legal consultation.

Attachments and Future MTAS Publication

This Hot Topic has focused on only a small number of issues pertinent to the monitoring of e-mail. Attachment I is a sample policy for the general use as well as monitoring of e-mail. It includes provisions on a large number of legal and personnel issues involved in those practices. The city may not need all of the provisions in the sample policy. But, if it decides to monitor, it should carefully consider each provision.

Reminder: Even if the city decides not to monitor e-mail, it must adopt a policy that contains at least a provision stating that employee's e-mail may be a public record and subject to inspection under Tennessee's Public Records Law (T.C.A. § 10-7-512).

MTAS will publish a comprehensive publication on the ethical, legal, and personnel issues involved in the use and monitoring of e-mail, including those mentioned in this Hot Topic. It will also provide reasons for each of the policies and procedures prescribed in Attachments I and II.

Bibliography

For the sample e-mail policy contained in Attachment I, the author gratefully credits Thompson, B.J. (1998 February). Ethics in the Information Age. Paper presented at a seminar for the Tennessee Municipal Attorney's Association, Nashville, Tennessee.

ATTACHMENT 1

Sample Policy for the Use and Monitoring of E-mail

1. Purpose and Scope

The city provides electronic mail (e-mail) to employees for their use in performing their duties for the city. These materials explain the city's rules and expectations for the proper use of electronic mail. This document also sets forth the city's policy with respect to when e-mail messages may be monitored by other people within the city, as well as the circumstances under which e-mail messages may be disclosed to persons outside the city administration. For example, access to e-mail may be granted to external users, such as other cities' employees, special task-force members, or pursuant to a lawful subpoena.

All electronic mail is a local government record and may be considered a "public record" for the purposes of the Tennessee Public Records Act. Under the Public Records Act, certain e-mail communications may be open to public access and inspection. In addition, such communications may be subject to discovery under the Tennessee or Federal Rules of Civil Procedure.

2. Background

Benefits of E-mail. The city finds that e-mail provides many benefits to the city and its employees. E-mail often improves communication between different departments, eliminates unnecessary paperwork, allows communication with many other governmental offices almost instantaneously, and generally facilitates the smooth operation of city services.

3. Ownership

All electronic systems, computers, and other hardware, software, temporary or permanent files, and any related systems or devices used in the transmission, receipt, or storage of e-mail are the property of the city of_____. E-mail messages are considered to be city property. Also, they may be retrieved from storage even after they have been deleted by the sender and the recipient.

4. Responsibilities

Records Manager. The city will designate a records manager or other individual who will be designated as a coordinator for public records generated by e-mail. It is the responsibility of this individual to accommodate members of the public who request access to e-mail. The records manager will also keep a log on the use of public access to the system and develop an efficient procedure to be used for public access to e-mail communications. The records manager may also provide and/or coordinate user training.

Individuals Requesting Access to E-mail. Depending on the circumstances and resources, searches requested pursuant to the Public Records Act will be made either by the requestor or a city representative. Any requestor claiming a qualified disability will be accommodated by the city in accordance with the Americans With Disabilities Act.

5. Statement of Policy and Overview of Usage

Policy. It is city policy that the e-mail system, like other city assets, is used only for the benefit of the city. Use of e-mail that violates city policies or state and/or federal law is prohibited and may lead to disciplinary action up to and including termination. All employees who use e-mail will certify that they have read and fully understand the contents of this policy by signing the attached acknowledgment. Any and all statements and opinions made by individuals using e-mail, whether implied or expressed, are those of the individual and not necessarily the opinions of the city or its management.

Privacy. Employees should be aware that e-mail messages may be read by others for a variety of valid reasons. Although this statement applies to many other types of city correspondence, the informal nature of e-mail may lead one to forget or ignore the fact that e-mail is considered to be the private property of the sender or the recipient, even if passwords or encryption codes are used for security reasons.

Monitoring. The city reserves the right to monitor messages under certain circumstances, as enumerated in this document. Supervisors have the authority to inspect the contents of any equipment, files, calendars, or electronic mail of their subordinates in the normal course of their supervisory responsibilities and without the express permission from the user(s). An individual qualified in data management shall extract stored e-mail messages when requested to do so by authorized supervisory personnel.

Reasons for monitoring or retrieving e-mail messages include the following:

- during the course of an investigation that has been triggered by indications of impropriety,
- when it is necessary to locate substantive information relevant to a breach of security of the e-mail system,
- at any time there may be system hardware or software problems,
- for regular system maintenance,
- any messages relevant to a lawsuit or other legal action involving the city, and
- a suspicion of a crime or a violation of this policy.

The city will disclose any e-mail message to law enforcement officials if legally required to do so. In addition, e-mail messages may be retrieved if there is a need to perform work or provide a service when the user-employee is unavailable.

Personal Use. Should employees make incidental use of e-mail to transmit personal messages, those messages will be treated no differently than other messages and may be accessed, reviewed, copied, deleted, or disclosed. You should not expect that a message will never be disclosed to or read by others beyond its original intended recipient(s).

Authorized Uses. Supervisors or department heads may authorize the use of e-mail to send and

receive messages and to subscribe to list-servers from recognized professional organizations and entities relating to the official duties of the city. All employees are authorized to use e-mail as they would any other official city communication tool. Communication by e-mail is encouraged when it results in the most efficient or effective means of communication.

Uses Subject to Approval. The following uses require the written approval of the employee's supervisor or department head:

- Using hardware, related computer equipment, and software not owned or purchased by the city for e-mail related to city business.

- Reading electronic mail of another employee without prior written approval. However, an employee's supervisor may inspect the contents of e-mail pursuant to the section entitled "Ownership" in this policy.

- Encrypting any e-mail message unless specifically authorized to do so and without depositing the encryption key with the computer administrator or your immediate supervisor prior to encrypting any messages. If an employee is allowed to encrypt e-mail, this does not mean that e-mail is intended for personal communication nor does it suggest that encrypted e-mail messages are the private property of the employee.

Prohibited Uses. The following actions are prohibited:

- intercepting, eavesdropping, recording, or altering another person's e-mail message;

- forwarding a message sent to you without the sender's permission, including chain letters;

- adopting the identity of another person on any e-mail message, attempting to send electronic mail anonymously, or using another person's password;

- misrepresenting yourself or your affiliation with the city in any e-mail message;

- composing e-mail that contains racial, religious, or sexual slurs or jokes, or harassing, intimidating, abusive, or offensive material to or about others;

- using e-mail for any personal commercial or promotional purpose, including personal messages offering to buy or sell goods or services;

- using e-mail to conduct employee organization, association, or union business; and

- sending or receiving any software in violation copyright law.

6. Confidential Information

Employees must exercise a greater degree of caution in transmitting confidential information via e-mail than with other forms of communications. Why? Because it paves the way for another person to redistribute such information almost effortlessly. Confidential information should never be trans-

mitted or forwarded to other employees inside or outside the city who do not have a "need to know." To reduce the chance that confidential information inadvertently may be sent to the wrong person, avoid misuse of distribution lists and make sure that any lists used are current.

If you are unsure whether certain information is confidential, consult your supervisor, your city attorney, or an MTAS legal consultant. Examples of information that either are or may be considered confidential include but are not limited to:

- certain personal information from a person's personnel file, including medical records about employees and personal, identifying information of undercover detectives, such as home addresses, telephone numbers, identities of family members, and Social Security numbers;
- information relating to an administrative hearing and litigation of a civil or criminal nature;
- information that, if released, would give a competitive advantage to one prospective bidder over another for city contracts;
- private correspondence of elected officials;
- trade secrets or commercial or financial information of outside businesses;
- information related to the regulation of financial institutions or securities;
- information regarding an ongoing criminal investigation; and
- taxpayer information.

E-mail messages that contain confidential information should have a confidentiality declaration printed at the top of the message in a form similar to the following:

"THIS MESSAGE CONTAINS CONFIDENTIAL INFORMATION OF THE CITY OF_____. UNAUTHORIZED USE OR DISCLOSURE IS PROHIBITED."

Since copies of e-mail may be backed up or sent to other systems, they can easily be retrieved later by information system personnel who should not know the content of the message. Therefore, employees should keep in mind that e-mail may **not** be the best form of communication with respect to certain types of confidential information.

Messages to Legal Counsel. All messages to and from legal counsel seeking or giving legal advice should be marked with the following legend in all capital letters at the top of the page:

"CONFIDENTIAL ATTORNEY/CLIENT PRIVILEGED INFORMATION."

In addition, to preserve the attorney/client privilege, messages to and from legal counsel should never be sent to distribution lists or forwarded to anyone else. It is best if such messages are not retained on a network e-mail system. If a copy of an attorney/client privileged communication needs to be retained, it should be printed and filed in an appropriate place.

7. Copyright Infringement

The ability to attach a document to an e-mail message for distribution may increase the risk of copyright infringement as prohibited by federal law. A user can be liable for the unauthorized copying and distribution of copyrighted material through e-mail systems. Accordingly, you should not copy and distribute by e-mail any copyrighted material of a third party, such as software, database files, documentation, articles, graphics files, and downloaded information, unless you confirm in advance from appropriate sources that the city has the right to copy or distribute such material. Any questions concerning these rights should be directed to appropriate legal counsel.

8. Retention of E-mail

Deletion of Messages. The city strongly discourages the local storage of large numbers of e-mail messages. Retention of messages takes up large amounts of storage space on the network server. In addition, because e-mail messages can contain confidential information, it is desirable to limit the number, distribution, and availability of such messages. Of course, if the message contains information that must be preserved as a permanent record, it must be saved and archived.

9. Policy Violations

Violations of this policy will be reviewed on a case-by-case basis and can result in disciplinary action up to and including termination. All e-mail messages are subject to all state and federal laws that may apply to the use of e-mail. In addition, violations of this policy or misuse of the e-mail system could result in civil or criminal prosecution.

ATTACHMENT 2

ACKNOWLEDGMENT

I hereby acknowledge that I have received and read a copy of the city of _____'s Policy for the Use and Monitoring of E-mail. I understand that all e-mail communications systems are the property of the city, as is the information received from, transmitted by, or stored in these systems. I understand that, except with respect to certain content deemed confidential by state and federal law, I have no expectation of privacy in connection with any e-mail messages, the use of city equipment, or the transmission, receipt, or storage of information in this equipment.

I acknowledge and consent to the city's monitoring my use of both Intranet and Internet e-mail at any time the city deems it necessary in accordance with its policy. Monitoring may include reading and printing out all electronic mail entering, stored in, or disseminated by the city of _____'s system and equipment. I agree not to use a code, access a file, or retrieve any stored information unless authorized to do so. I understand that this consent is a condition of my employment and/or continued association with the city. I understand all the provisions specified in this policy. Further, I recognize that a violation of this policy may result in disciplinary action, including possible termination.

_____

Employee

_____

Supervisor/Employer

_____

Date

Frances Adams-O'Brien
MTAS Knoxville

The University of Tennessee
Institute for Public Service
105 Student Services Building
Knoxville, TN 37996-0213

The Municipal Technical Advisory Service (MTAS) is a statewide agency of The University of Tennessee's Institute for Public Service. MTAS operates in cooperation with the Tennessee Municipal League in providing technical assistance services to officials of Tennessee's incorporated municipalities. Assistance is offered in areas such as accounting, administration, finance, public works, communications, ordinance codification, and wastewater management.

MTAS *Hot Topics* are information briefs that provide a timely review of current issues of interest to Tennessee municipal officials. *Hot Topics* are free to Tennessee local, state, and federal government officials and are available to others for $2 each. Photocopying of this publication in small quantities for educational purposes is encouraged. For permission to copy and distribute large quantities, please contact the MTAS Knoxville office at (865) 974-0411.

Printed on Recycled Paper.